Parcimonie et inversion à gauche : le cas des cyber-attaques

J-P Barbot et al.

QUARTZ laboratoire

November 14, 2017

Plan

- Introduction
- Rappels sur l'utilisation de la parcimonie
- Présentation de l'algorithme
- Utilisation de la parcimonie dans un contexte Cyber-Attaques
- Conclusion

Introduction

Si on regarde les thématiques de ‘’notre GT”, un grand nombre de questions surgissent :

- Différences entre Observation et Synchronisation
- Différences entre Observateur, filtre, différentiateur
- Différences entre Observateur à entrées inconnues et inversion à gauche
- Différences entre Inversion à gauche et estimation paramétrique
- ...

Introduction

Si notre domaine d'expertise se différentie facilement de celui des cryptologues, physiciens, mathématiciens, ...
Notre proximité avec les traiteurs de signaux est beaucoup plus affirmée.
Voir historiquement le filtre de Kalman et l'Observateur de Kalman-Bucy.
Notre différence principale est pour l'un, une plus grande prise en compte du système qui a produit le signal et pour l'autre une plus grande prise en compte des propriétés du signal.

Introduction

Mais peut-on tirer parti de ces deux approches ?
C'est ce qui va être illustré dans la présentation qui suit sur l'exemple de la parcimonie, une information qui sort du simple cadre système et signal
Les harmoniques, les ondelettes, . . . peuvent être considérés parcimonieux et cela a donné au Compressive Sensing
les attaques, les défauts peuvent être considérés parcimonieux et cela pourrait donner lieu à de nouveaux développement en Diagnostic et en Cyber-attaques.

Rappels sur l'utilisation de la parcimonie

Considérons le problème suivant:

$$y = \Phi x + \varepsilon \tag{1}$$

où $y \in \mathbb{R}^M$, $x \in \mathbb{R}^N$, ε est le bruit de mesure et $N >> M$ avec $Rank(\Phi) = M$.
Une solution sans bruit ($\varepsilon = 0$) est envisagable sous forme de la matrice pseudo inverse de Moore-Penrose :

$$\bar{x} = \Phi^T(\Phi\Phi^T)^{-1}y \tag{2}$$

Mais ce n'est qu'une solution.

Rappels sur l'utilisation de la parcimonie

Il nous faut faire une hypothèse supplémentaire :

Definition

La matrice x est parcimonieuse si le nombre s d'éléments de x diffèrents de zéro est très inférieure à M.

Nous avons besoin de faire une hypothèse sur s

Assumption

$$s \leq \lfloor \frac{M-1}{2} \rfloor \tag{3}$$

Rappels sur l'utilisation de la parcimonie

Nous pouvons écrire le problème comme un problème d'optimisation

$$x^* = arg\,min_{x \in R^N} \{ \frac{1}{2} ||y - \Phi x||_2^2 + \lambda ||x||_0 \} \qquad (4)$$

avec $\lambda > 0$, mais l'optimisation par rapport à la norme zéro est un problème ouvert.

Rappels sur l'utilisation de la parcimonie

Il nous faut une hypothèse supplémentaire, celle-ci est faite sur la matrice Φ (Candès, Donoho, Tao), c'est la RIP (Restricted Isometry Property)

Assumption

La matrice Φ vérifie la RIP à l'ordre s avec une constante $\delta_s \in (0,1)$ c.-à-d.

$$(1-\delta_s)||x||_2^2 \leq ||\Phi x||_2^2 \leq (1+\delta_s)||x||_2^2 \tag{5}$$

$\forall x \in \Gamma$ *avec* $\Gamma = \{x / ||x||_0 \leq s\}$.

Rappels sur l'utilisation de la parcimonie

Sous cette hypothèse le problème d'optimisation devient

$$x^* = arg\,min_{x \in R^N} \{ \frac{1}{2} ||y - \Phi x||_2^2 + \lambda ||x||_1 \} \qquad (6)$$

est il y a unicité de la solution.

Présentation de l'algorithme

Pour que notre algorithme puisse être inséré dans une boucle temps réel continue, nous proposons l'algorithme suivant :

$$\begin{cases} \tau \dot{u} &= -\lceil u + (\Phi^T \Phi - I)a - \Phi^T y \rfloor^\alpha \\ a &= T_\lambda(u) := max(|u| - \lambda, 0) sgn(u) \end{cases} \tag{7}$$

avec

$$\lceil . \rfloor^\alpha := |.|^\alpha sgn(.)$$

et $\hat{x} = 0$ si $a = 0$ sinon $\hat{x} = a + \lambda sgn(a)$.

Présentation de l'algorithme

Theorem

Sous l'hypothèse que Φ est s-RIP (Assumption 2 et 3) le système (7) converge ''globalement" vers u^*, a^* et x^*.

Remarque

Si $\alpha = 1$ on est linéaire et on a exactement le Locally Competitive Algorithm (LCA), qui ne garantit pas une convergence en temps fini. Si $\alpha = 0$ la dynamique des Neurones est alors un sliding mode d'ordre 1.

Présentation de l'algorithme

Lemme

Les point d'équilibres de (7) sont les solutions du problème d'optimisation de ((6) (i.e. (4)).

Idée de preuve:

$$\frac{\partial \frac{1}{2}||\Phi u - y||_2^2 + \lambda||u||_1}{\partial u} = (\Phi^T(\Phi u - y) + \lambda sgn(u))^T$$

et de T_λ on a $u - x = \lambda' sgn(u)$ avec $\lambda \in (0, \lambda]$, on a

$$\frac{\partial \frac{1}{2}||\Phi u - y||_2^2 + \lambda||u||_1}{\partial u} = (\Phi^T(\Phi(u - x) + k'(u - x))^T$$

avec $k' \in (0, 1]$. $\dot{u} = 0$ sont les points singuliers de (6).

Présentation de l'algorithme

Lemme

Le système (7) est partout intégrable et a une solution unique et aucun phénomène de Zénon apparait.

Lemme

Pour toute condition initiale de u bornée, la trajectoire (7) reste confinée dans un bornée.

Idée de preuve:

$$V(u) = \frac{1}{2}||y - \Phi T_\Lambda(u)||_2^2 + \lambda||T_\lambda(u)||_1$$

$\dot{V} \leq 0.$

Présentation de l'algorithme

Remarque

Même si le théorème de LaSalle demande que la dynamique évolue dans un bornée comme ce bornée peut être choisie aussi grand que l'on veut en fonction de la condition initiale, nous considérerons la convergence obtenue comme "Globale".

Présentation de l'algorithme

Afin, de prouver la convergence de (7), nous définissons les termes d'erreur suivants $\tilde{u} = u - u^*$ et $\tilde{a} = a - a^*$ et la fonction de "Lyapunov" suivante :

$$E(u) = \frac{1}{2}||\tilde{u}||_2^2 + 1^T(\Phi^T\Phi - I)G(\tilde{u})$$

avec $G(\tilde{u}) := (G_1(\tilde{u}_1), ..., G_N(\tilde{u}_N))^T$ où

$$G_i(\tilde{u}_i) = \int_0^{\tilde{u}_i} g_i(s)ds \qquad \text{et} \qquad g_i(s) = T_\lambda(s + u_i^*) - T_\lambda(u_i^*)$$

Présentation de l'algorithme

Lemme

La fonction E et la dynamique (7) satisfont les propriétés suivantes :

- $\forall \tilde{u}_i$, *on a* $0 \leq G_i(\tilde{u}_i) \leq \frac{\tilde{u}_i}{2}$
- $\dot{E} \leq 0$
- $0 \leq E$
- *Il existe une constante* $\nu > 0$ *telle que*

$$E(\tilde{u}) \leq \nu ||\tilde{u}||_2^2$$

Présentation de l'algorithme

Theorem

Sous l'hypothèse de s-RIP (Assumption 2 et 3) la dynamique (7) converge "globalement" vers le point critique de (6) (i.e. (4)).

Idée de preuve:
Théorème de LaSalle et le seul point invariant est le point critique de (6) (i.e. (4)).

Présentation de l'algorithme

Lemme

Il existe un temps t_e et une constante $\kappa > 0$ tels que $\forall t > t_e$

$$\kappa ||\tilde{u}||_2^2 \leq ||\tilde{u} + (\Phi^T \Phi - I)\tilde{a}||_2^2$$

Présentation de l'algorithme

Le temps maximal de convergence $t_f(E_0)$ est

$$t_f(E_0) = \frac{2E_0^{\frac{1-\alpha}{2}}}{\theta^{\frac{1+\alpha}{2}}(1-\alpha)}$$

avec $E_0 := E(\tilde{u}(0))$ et $\theta = \frac{\kappa}{\nu}$.

Utilisation de la parcimonie dans un contexte Cyber-Attaques

Le réseau électrique peut être modélisé par le système d'équations algébro-differentielle suivant :

$$\begin{bmatrix} I & 0 & 0 \\ 0 & M_g & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} \omega \\ P_g^e - P_g^{n\omega}(\theta, V) - E_g\omega \end{bmatrix} + Bu$$
$$y = g(x) + Du \tag{8}$$

Avec $\omega \in \mathbb{R}^p$ les pulsations dans le réseau, $\delta \in \mathbb{R}^p$ les angles dans le réseau, $\theta \in \mathbb{R}^q$ déphasage par rapport à la tension de bus, $V \in \mathbb{R}^\kappa$ les tensions de bus, $y \in \mathbb{R}^M$ les sorties capteurs et $u \in \mathbb{R}^N$ est le vecteur des attaques.

Utilisation de la parcimonie dans un contexte Cyber-Attaques

Après transformation le système d'équation algébro-différentielle devient

$$\begin{aligned} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} &= \begin{bmatrix} \phi_\delta(\delta,\omega) \\ \phi_\omega(\delta,\omega) \end{bmatrix} + \begin{bmatrix} 0 \\ P_{\theta,\omega} \end{bmatrix} + \begin{bmatrix} B_\delta \\ B_{\theta,\omega} \end{bmatrix} u \\ y &= G_0 \begin{bmatrix} \delta \\ \omega \end{bmatrix} + D_0 u \end{aligned} \tag{9}$$

On fait l'extension dynamique suivant

$$\dot{z} = \frac{1}{\tau}(-z + G_0 \begin{bmatrix} \delta \\ \omega \end{bmatrix} + D_0 u)$$

Utilisation de la parcimonie dans un contexte Cyber-Attaques

Nous prenons M fonctions $\psi_i(z, \dot{z}, \ldots, z^{(l)})$ telles que

$$\begin{bmatrix} \psi_1(z, \dot{z}, \ldots, z^{(l)}) \\ \vdots \\ \psi_M(z, \dot{z}, \ldots, z^{(l)}) \end{bmatrix} = F(z, \dot{z}, \ldots, z^{(l-1)})u$$

avec $F(z, \dot{z}, \ldots, z^{(l-1)})$ qui doit vérifier la s-RIP.

Utilisation de la parcimonie dans un contexte Cyber-Attaques

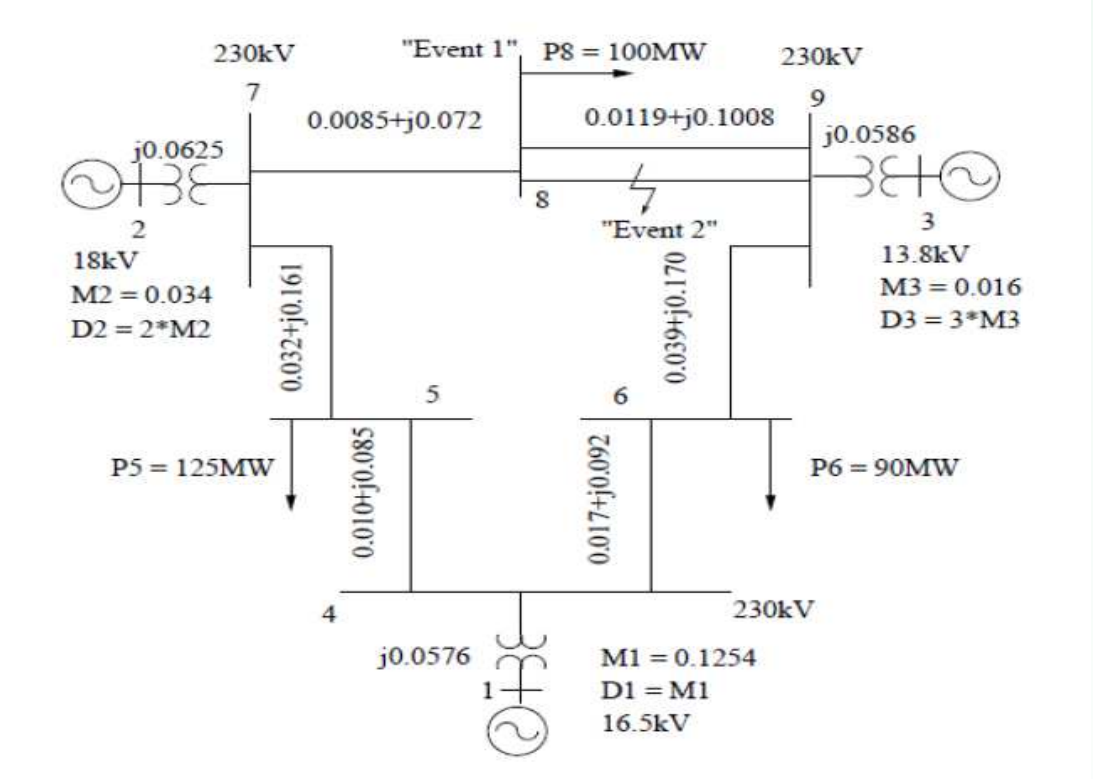


Figure: The Western Electricity Coordinating Council Power System.

Utilisation de la parcimonie dans un contexte Cyber-Attaques

$$\tilde{F} = \begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 8 & 0 & 0 & 3.96 & 1.88 & 1.96 & 2.60 & 2.66 & 1.93 & 0.31 & -0.12 & -0.11 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 29.41 & 0 & 7.52 & 15.96 & 6.96 & 13.04 & 7.16 & 10.71 & -0.44 & 0.85 & -0.41 & 0 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & 62.50 & 15.59 & 13.86 & 32.36 & 14.46 & 26.47 & 24.66 & -0.90 & -0.87 & 2.40 & 0 & 0 & -3
\end{bmatrix}$$

Figure: F Matrix, in steady state.

Utilisation de la parcimonie dans un contexte Cyber-Attaques

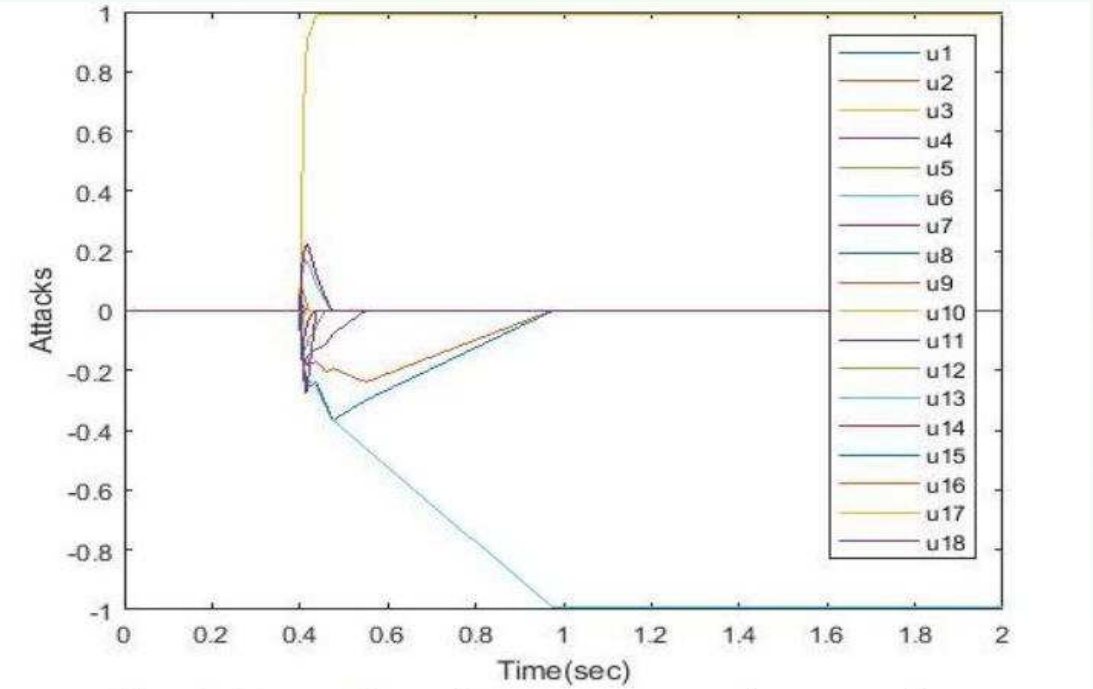


Fig. 2: Detection of two constant plant attack

Utilisation de la parcimonie dans un contexte Cyber-Attaques

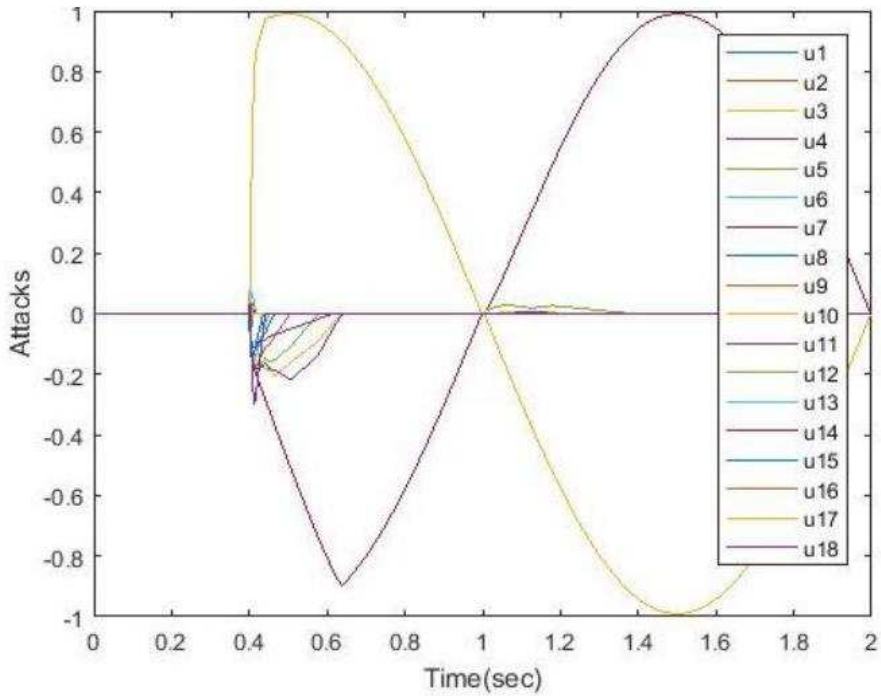


Fig. 3: Detection of two time varying plant attack

Utilisation de la parcimonie dans un contexte Cyber-Attaques

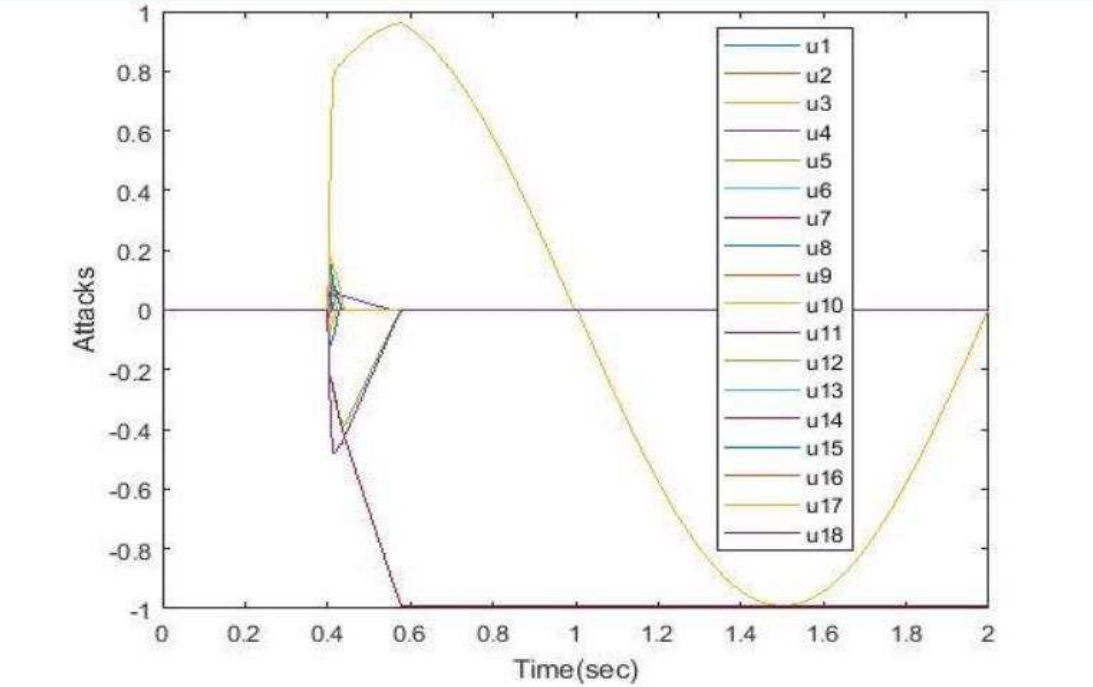


Fig. 4: Detection of time varying plant attack and sensor constant attack

Conclusion

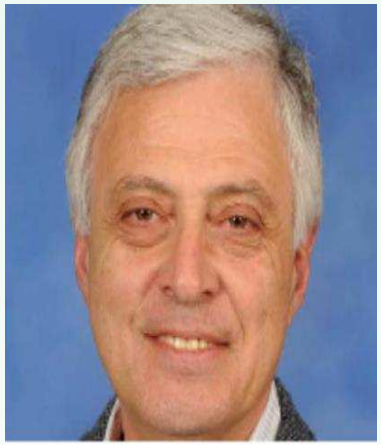
- Pour des matrices qui ne sont pas quasi constantes
- Pour du diagnostic
- Pour des matrices faiblement RIP

Contributeurs

Gang Zheng

Lei Yu

Malek Ghanes



Yuri Shtessel

Shamila Nateghiboroujeni

Junying Ren

Références

H. Alwi, C. Edwards and C.P. Tan, “Fault detection and fault-tolerant control using sliding modes”, Springer, 2011.
A. Balavoine, C. J. Rozell and J. Romberg, “Discrete and continuous-time soft-thresholding for dynamic signal recovery” IEEE Trans. on Signal processing, 2015.
J-P. Barbot, D. Boutat and T. Floquet, “An observation algorithm for non-linear systems with unknown inputs”, Automatica, 2009.
S. P. Bath and D. S. Berstein, “Finite-time stability of continuous autonomous system”, SIAM JCO, 2000.
E. Candès and T. Tao, “The dantzig selector: Statical estimation when *p* is much larger than *n*", The Annals of Statistics, 2007.
K. M. Hirschorn, “A note on the invertibility of nonlinear input-output differential systems”, IEEE TAC, 1979.

Références

S. Nateghi, Y. Shtessel, J-P. Barbot, L Yu, G. Zheng, “Cyber-attacks reconstruction in electrical power networks via sparse recovery algorithm and sliding modes", submitted for publication

F. Pasqualetti, F. Dörfler and F. Bullo, “Attack detection and identification in Cyber-Physical system", IEEE TAC, 2013.

W. Respondek, “Right and left invertibility of nonlinear control systems", Nonlinear controllability and optimal control, 1990.

L. Yu, G. Zheng and J-P. Barbot, “Dynamic sparse recovery with finite-time convergence", IEEE Transaction on Signal Processing, 2017.